

**Listing of Claims**

1. (Currently Amended) A method for checksum generation and utilization, in an apparatus for performing modulo  $N$  multiplication of integers  $A$  and  $B$  in which said modulo multiplication is carried out in  $k$  bit wide portions of the factors  $A$  and  $B$  which are representable and as  $\sum_{i=0}^{m-1} A_i R^i$  and  $\sum_{i=0}^{m-1} B_i R^i$  where  $R$  equals  $2^k$  and where  $N$  is representable as  $\sum_{i=0}^{m-1} N_i R^i$ , said method comprising the steps of:

operating said multiplication apparatus over a plurality of cycles so as to produce, at each cycle  $i$ , the values  $Z_i$  and  $Y_i$  in accordance with a two phase modular multiplication method which does not require division operation;

accumulating, over said cycles, sums modulo  $(R - 1)$  of the values  $A_i [Ai]$ ,  $B_i$ ,  $N_i$ ,  $Y_i$  and  $Z_i$ ; and

comparing the sum of the  $Z_i$  values with the sum of two products, the first product being the product of the sums of the  $A_i$  and  $B_i$  terms, and the second product being the product of the sums of the  $N_i$  and  $Y_i$  terms.